~~SECRET~~

15 JUL 1986

MEMORANDUM FOR: See Distribution

FROM: [redacted] 25X1
Executive Officer
Office of Security

SUBJECT: Request for Comments on Proposed National Security Decision Directive (NSDD) on Operations Security (OPSEC) [redacted] 25X1

ATTACHMENT: Proposed NSDD [redacted] 25X1

1. In February 1986, component comments were solicited regarding a proposed National Security Decision Directive (NSDD) on Operations Security (OPSEC). Shortly after comments were received, work on the NSDD was suspended by the National OPSEC Advisory Committee (NOAC) pending reorganization of the interagency structure which deals with security countermeasures. That reorganization being complete and the NOAC retaining its former functions, the issue of promulgating a national OPSEC policy is once again before us in the form of the original NSDD, modified only to reflect the new structure. [redacted] 25X1

2. Because OPSEC is a term and a discipline unfamiliar to many CIA managers, a bit of background may be helpful: OPSEC concentrates on identifying things which opposition services might observe, which might serve to betray the presence or substance of a U.S. classified activity. Such "observables" could include the size and shape of a building, conversations on an open telephone line, antenna configuration, etc. Of course, CIA practices operational security in many forms, not the least of which is Tradecraft. [redacted] 25X1

3. However, a comprehensive OPSEC program is truly multidisciplinary and requires coordination among intelligence collectors and analysts, counterintelligence and counterimagery personnel, technical and personnel security specialists, communications personnel, and program planners and managers. While OPSEC surveys can be conducted by security personnel, they require multidisciplinary expertise to develop and the OPSEC product is ultimately, like security, the responsibility of program and line managers. [redacted] 25X1

25X1

[redacted]

~~SECRET~~

25X1

4. The proposed NSDD has several implications for CIA. It would:

° require an annual report on the status of OPSEC in CIA. We have been assured that this would be a very general report and that sensitive sources and methods information would not be required (we are not sanguine that this would be the case - see paragraph #6 below). 25X1

° have at least some minimal resource implications. We would have to provide a representative to the Interagency OPSEC Support Staff, develop at least a semblance of an OPSEC program, and distribute OPSEC educational materials. [redacted]

[redacted]

6. Comments on the earlier version of the NSDD were largely noncommittal except for strong feelings that a sources and methods "carve-out" should be explicitly included. The following exclusionary language was suggested: "Nothing in this Directive: (a) alters the authorities of the DCI to protect intelligence sources and methods or of any authorized agency or department to conduct intelligence-related activities nor (b) implies any authority to examine the facilities or operations of any department or agency without the approval of the head of such agency or department." [redacted]

7. The focal point in CIA for interagency OPSEC matters has been the Office of Security due to the Director of Security's position as CIA representative to NOAC's parent organization, the Interagency Group/Countermeasures(Policy) (IG/CM(P). Requested are your views on how (or if) OPSEC might be handled within CIA as well as your comments on the proposed NSDD. Please respond by 24 July as the combined response is due to the IG/CM(P) on 29 July.

[redacted]

25X1

25X1

Distribution:
C/CI Staff/DDO
C/Imagery Group/CRES/DDI
C/FICG/OGI
C/CSD/OC
NIO/FDIA
C/SMS/DDS&T
DD/PS
C/CI&SG
C/CG
C/IG
DD/PTS
C/PSS/PTS
¦EO/OS¦
¦PPG Chrono¦
¦OS Registry¦

¦OS/EO/PPS [redacted] (15 Jul 86)¦ 25X1

ATTACHMENT 3

National Security Decision
Directive Number ________

NATIONAL OPERATIONS SECURITY PROGRAM

BACKGROUND

The national security requires that all departments and agencies of the United States Government shall plan for and execute operational security (OPSEC) measures, permitted by law and policy, to deny adversaries information concerning classified activites. Effective security measures currently exist to protect classified activities and information; however, exploitable unclassified activities and information can often compromise classified US Government operations, programs, and projects. Such activities and information are hereinafter considered sensitive.

Operations security (OPSEC) is a process intended to deny information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and execution of government activities. Application of OPSEC involves a process of analysis of an activity or program to determine needed security modifications that will result in adequate protection.

The key elements of the OPSEC process are:

a. Functional analyses of a program to identify the specific information or activity that must be protected or controlled.

b. Analyses of "observable" activity and information to identify exploitable characteristics.

c. Threat analyses to determine applicable hostile intelligence capabilities, interests, and opportunities.

d. Assessments to determine the relative significance of specific vulnerabilities and what countermeasures can be implemented.

e. Implementation of countermeasures which respond to specific vulnerabilities during the planning and execution of a government activity or program.

POLICY

A National Operations Security Program is hereby established. Each department and agency involved directly or indirectly with classified or sensitive activities shall establish a formal OPSEC program, the common features of which are:

a. Application and direction of OPSEC by program managers or commanders.

b. Positive measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.

c. Responsiveness to the OPSEC concerns of other departments and agencies.

d. A requirement to present an annual general OPSEC status report to the National OPSEC Advisory Committee (defined below). The report will outline a department or agency's OPSEC program, highlighting pertinent success and problem areas which may aid others with their OPSEC programs.

COORDINATION

The Interagency Group/Countermeasures (Policy) (IG/CM(P)), National Operations Security Advisory Committee (NOAC), chaired by a representative of the Secretary of Defense, with membership from each of the departments and agencies participating in the IG/CM(P) and with other departments and agencies invited as appropriate shall serve as the principal interagency forum within the executive branch for discussion, consultation, and coordination of OPSEC issues. The NOAC shall advise the IG/CM(P) concerning OPSEC policies and procedures to be recommended to member departments and agencies to protect sensitive programs and activities. Under the guidance of the IG/CM(P), the NOAC shall:

a. Bring to the attention of the IG/CM those OPSEC vulnerabilities and deficiencies the NOAC may identify within sensitive programs and activities of the executive branch.

b. Provide the IG/CM(P) with advice and recommendations concerning measures and methods for reducing OPSEC vulnerabilities and corrective measures.

c. As requested, consult with, and provide advice and recommendations to, the various departments and agencies of the executive branch concerning OPSEC vulnerabilities and corrective measures.

d. Coordinate OPSEC support among the various departments and agencies within the executive branch when interagency coordination is appropriate and necessary.

e. Prepare OPSEC studies, analyses, advisory memoranda, recommendations, and informational materials for consideration and use by the various departments and agencies of the executive branch.

f. As requested, review and provide comments, advice, and recommendations concerning OPSEC policies and procedures in effect within and among the various departments and agencies of the executive branch.

SUPPORT

The Director, National Security Agency is designated as the executive agent for OPSEC training, is tasked to develop and provide OPSEC training courses, shall establish and maintain an Interagency OPSEC Support Staff (IOSS), the membership of which shall include, as a minimum, a representative of the Central Intelligence Agency, the Federal Bureau of Investigation, the Department of Defense, and the Department of Energy. The IOSS will:

a. Carry out OPSEC training for executives, program and project managers, and OPSEC specialists of the departments and agencies.

b. Assist the departments and agencies, as needed, to set up their own OPSEC programs, act as consultants for OPSEC surveys and analysis, sponsor research and development of advanced OPSEC technologies, and develop and deliver OPSEC training programs.

c. Provide a technical staff for the NOAC.

DEFINITIONS. As used herein, the term:

a. Operations Security (OPSEC): Refers to the process of identifying, controlling, and protecting indicators--associated with the planning and execution of government activities--to deny adversaries accurate estimates of classified or sensitive activities and information. Application of OPSEC involves a process of analysis of a program, project, or office, to determine needed security modifications that will result in adequate protection.

b. Sensitive Activities: Refers to operations, investigations, inquiries, tests, research, training, exercises, and other functions of departments and agencies, or their contractors, where the disclosure of such to adversaries could reasonably be expected to damage the national security.

c. Indicators: Refers to inferences from open source data which can be gleaned from administrative, physical, and technical actions necessary to plan, prepare for, and execute government activities.

CCISCMS/ICS [redacted] STAT

Distribution of D/ICS-86-0851 (w/att as shown):

1 - Mr. Alderman, OSD
1 - Mr. Snider, OSD
1 - Mr. Donnelly, ODUSD(P) (via Mr. Snider)
1 - Mr. Anderson, ODUSD(P) (via Mr. Snider)
1 - Mr. Latham, ASD C^{3}I
1 - Mr. Dill, OACSI, DA
1 - Mr. Flynn, Navy
1 - Mr. Cornett, Air Force
1 - Mr. Guenther, Marine Corps
1 - Mr. Seidman, Coast Guard
1 - [redacted] DIA STAT
1 - NSA
1 - Mr. DuHadway, FBI
1 - Mr. Corry, State
1 - Mr. Lamb, State (via Mr. Corry)
1 - Mr. Major, NSC
1 - [redacted] CIA STAT
1 - CIA (via [redacted]
1 - Ms. Lawton, DoJ
1 - Mr. Jackson, Commerce
1 - Mr. Badolato, Energy
1 - Mr. McBrien, Treasury
1 - Mr. Garfinkel, ISOO
1 - ICS Registry STAT
1 - IG/CM subject
1 - IG/CM chrono